UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,857	05/13/2005	Sebastien Canard	33901-175PUS	7415

27799 7590 09/11/2008

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
SHEPELEV, KONSTANTIN	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/534,857	CANARD ET AL.	
	Examiner	Art Unit	
	KONSTANTIN SHEPELEV	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/13/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on May 13, 2005 in which claims 1-19 are presented for examination.

Status of Claims

Claims 1-19 are pending; of which claims 1 and 15 are in independent form. Claims 1-19 are rejected under 35 USC 103(a).

Information Disclosure Statement

1. The information disclosure statement filed 9/5/2008 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Objections

2. Claims 16-19 are objected to because of the following informalities: With respect to claim 16 recites a "method according to claim 15", while claim 15 is directed to a system. Examiner interprets that the method recited in claim 16 is a misprint and the claim should instead recite "a system". With respect to claims 17-19, they are objected to in view of the same reasons as stated in the objection to claim 16. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1).

With respect to claim 1, Teper teaches the limitation of "identifying and registering a client (C) and providing him with means for authenticating himself to an anonymous certification authority (ACA)" (column 2, lines 57-62) as users and Service Providers that wish to make use of the Online Brokering Service initially register with the Brokering Service, and in turn provided with the client and server software components needed to make use of the Brokering Services.

In addition, Teper teaches the limitation of "authenticating the client to the anonymous certification authority using the means provided in step i) and supplying means enabling him to authenticate himself anonymously to a server (Se)" (column 2, line 62 – Column 3, line 4) as users provide various account information to the Online Broker. This information is maintained in a brokering database at the Online Broker site, and is not exposed to the Service Providers (SP). Each user additionally selects a password, and is assigned a unique ID which can be mapped to the user only by the Online Brokering Service. The password and unique ID are stored in the brokering database, and are used to authenticate registered users. Where, (column 5, lines 26-37) users are in turn provided with the software component needed to make use of the

services offered by the broker providing the features of a pass-through authentication protocol which allows the registered user to be authenticated by the Online Broker upon accessing a Service Provider site while remaining anonymous to the Service Providers and the other entities of the distributed network.

Finally, Teper teaches the limitation of "authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with a server (Se)" (column 3, lines 5-13) as when a user connects to a registered SP site and attempts to access an online service, the SP site initiates a challenge-response authentication sequence which allows the Online Brokering Service to authenticate the user for the SP site. Furthermore, (column 3, lines 31-34) upon determining that a user is authentic, the Online Brokering Service preferably sends an anonymous session ID to the SP site to allow the SP site to anonymously bill the user for services subsequently purchased.

It is noted, however, that Teper does not explicitly teach the limitation of "selectively allowing contact between the server (Se) and the anonymous certification authority (ACA) to revoke the anonymity of the client (C) using the signature provided in step iii)."

On the other hand, Camnisch teaches the abovementioned limitation (page 3, paragraph 0028) as none of the credentials reveal any information about the user's real identity or pseudonym. However, the showing of credentials can be carried out in such a way that a designated revocation manager can later find the user's identity and/or pseudonym.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Camnisch into the system of Teper to allow the service

provider to reveal a real identity of the user if needed for further prosecution (Camnisch, page 3, paragraph 0028).

With respect to claim 2, Teper teaches the limitation of "before the step ii), an additional step of communication between the anonymous certification authority (ACA) and the server (Se) whereby the server (Se) presents to said authority (ACA) a request to obtain means enabling verification of the anonymous authentication supplied by a client (C)" (column 6, lines 14-20) as the Service Provider registers with the Broker by providing various business and payment information, and by entering a contract with the Broker. The Broker issues a password to the Service Provider, and provides a Service Provider with the server-side software components of the system.

5. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) as applied to claim 1 above, and further in view of Feig et al. (US 2002/0085713 A1).

With respect to claim 3, it is noted that neither Teper nor Camnisch teach the limitations of "a first stage in which the client (C) calculates data formed of a series of tokens of which one enables a session to be opened and the others enable that session to be maintained", "a second stage in which the client (C) makes a strong undertaking to the server as to the series of tokens", and "a third stage of maintaining the session with the aid of the series of tokens."

On the other hand, Feig teaches the abovementioned limitation (page 1, paragraph 0005) as sending server partitions the media file into a plurality of sequential data blocks. Thereafter,

the server generates a plurality of cryptographic token keys, each token key corresponding to one of the plurality of sequential data blocks. Then the server encrypts each respective one of the plurality of sequential data blocks using a corresponding token key, thereby producing a plurality of the encrypted sequential data blocks. Then the server transfers the encrypted sequential data blocks to the client receiver. At the same time, the server transfers the plurality of token keys to the client receiver for immediate or later use.

It would have been obvious to one of the ordinary skill in the art at the time of the invention that the method described above can be applied to transferring data from any one machine to any other machine, therefore it can be used to transfer data from client to server. Therefore, it would have been obvious to one of the ordinary skill in the art to incorporate teachings of Feig into the system of Teper and Camnisch to guarantee the secure and sequential delivery of the data.

With respect to claim 4, it is noted that neither Teper nor Feig explicitly teach the limitation of "all the tokens are for one-time use and strongly interdependent."

On the other hand, Camnisch teaches the abovementioned limitation (Abstract) as a refinement of the credential system provides credentials for unlimited use, so called multiple-show credentials, and credentials for one-time use, so called one-show credentials.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Camnisch into the system of Teper and Feig to prevent the re-use of digital credentials by an unauthorized party.

6. Claims 5, 6, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) and Feig et al. (US 2002/0085713 A1) as applied to claim 3 above, and further in view of Aiello et al. (US 6,397,329 B1).

With respect to claim 5, it is noted that neither of Teper, Camnisch, and Feig teach the limitation of "the token generation step uses two cryptographic primitives, namely a hashing function and a random number."

On the other hand, Aiello teaches the abovementioned limitation (column 4, lines 51-52) as for a certificate that is valid for D days (or other time period), the random number is hashed D times.

In addition, examiner takes and Official Notice that the process of generating digital tokens and signatures through the use of one-way hash function applied to the random number is known in the art. Therefore, it would have been obvious to one of the ordinary skill in the art to incorporate teachings of Aiello into the system of to generate the digital certificates.

With respect to claim 6, Aiello teaches the limitation of "the first token is obtained by applying the hashing function to the random number, the second token is obtained by applying the hashing function to the first token obtained, and so on until n tokens are obtained: H(Wo) = Wi H(Wn-I) = W" (Abstract) as cryptography device receives the token and performs a one-way function, such as a hash function, on this received token a certain number of times to obtain the Dth value.

With respect to claim 8, Aiello teaches the limitation of "information such as a numerical value is associated with the initialization token" (column 6, lines 37-38) as each node in the path has a unique value associated with it called the token value.

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) and Feig et al. (US 2002/0085713 A1) as applied to claim 3 above, and further in view of Sako (US 2001/0011351 A1).

With respect to claim 7, it is noted that neither of Teper, Camnisch, and Feig explicitly teach the limitation of "the second stage includes obtaining an anonymous signature of an initialization token W~ enabling authentication of a client by the server."

On the other hand, Sako teaches the abovementioned limitation (Abstract) as the reception subsystem determines whether received data is anonymous participation data authorized by the participant subsystem and further determines whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper, Camnisch, and Feig to allow the participants to participate anonymously.

8. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) and Feig et al. (US

2002/0085713 A1) as applied to claim 3 above, and further in view of Rupp et al. (US 2001/0027431 A1).

With respect to claim 9, it is noted that neither of Teper, Camnisch, and Feig teach the limitation of "A method according to claim 3, characterized in that on each new authentication the client (C) sends the server (Se) a token of at least one unit lower rank than that Previously used."

On the other hand, Rupp teaches the abovementioned limitation (page 3, paragraph 0033) as in a reverse auction, bid prices start high and move downward as bidders interact to establish a closing price.

Examiner takes the official notice that it is known in the art to use tokens to represent the monetary value, therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Rupp into the system of Teper, Camnisch, and Feig to provide an additional functionality to the anonymous bidding system described by Teper, Camnisch, and Feig.

With respect to claim 10, it is noted that neither of Teper, Camnisch, and Feig teach the limitation of "on each new authentication the client (C) sends the server (Se) a token Wi whose rank (i) is selected to be representative of the value of an operation, for example a number of bid increments"

On the other hand, Rupp teaches the abovementioned limitation (page 2, paragraph 0021) as method includes receiving initial values for each bid variable, and later receiving an updated value for one of the bid variables.

Examiner takes the official notice that it is known in the art to use tokens to represent the monetary value, therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Rupp into the system of Teper, Camnisch, and Feig to provide an additional functionality to the anonymous bidding system described by Teper, Camnisch, and Feig.

9. Claims 11, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) as applied to claim 1 above, and further in view of Sako (US 2001/0011351 A1).

With respect to claim 11, it is noted that neither Teper nor Camnisch teach the limitation of "it is applied to bidding and the steps of the client (C) submitting an increased bid are effected by sending successive tokens of lower rank"

On the other hand, Sako teaches the abovementioned limitation (page 4, paragraph 0069) as in the case where this anonymous participation authority management system is applied to a bidder management system of electronic bidding; the participant subsystem corresponds to a bidder subsystem and each eligible bidder is given secret information from the manager subsystem beforehand and the reception subsystem performs bidding reception.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch to provide additional functionality such as bidding application.

With respect to claim 12, it is noted that neither Teper nor Camnisch explicitly teach the limitation of "using a group signature by associating a plurality of identifiers and respective private keys with a single group public key."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0015) as the verification subsystem confirms that the data submitted has a signature verifiable by a group public key affixed and when the confirmation is obtained, this can be regarded as the data sent by a participant subsystem belonging to an eligible group.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch because use of the group signature makes it impossible to identify the particular participant in the group, which makes it possible to maintain anonymity.

With respect to claim 13, it is noted that neither Teper nor Camnisch explicitly teach the limitation of "using a blind signature."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0005) as a participant subsystem authorized to vote proves before a manager subsystem that the presenter is authorized to vote and then has the manager subsystem sign the voting contents by section of blind signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch because since blind signature is used, even the manager subsystem cannot know to which participant subsystem

the voting statement with the signature has been issued, which makes it possible to maintain anonymity.

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) in view of Camnisch et al. (US 2002/0103999 A1) and Sako (US 2001/0011351 A1) as applied to claim 12 above, and further in view of Beaver et al. (US 7,234,059 B1).

It is noted that neither of Teper, Camnisch, and Sako explicitly teach the limitation of "the powers to revoke anonymity are divided between two or more authorities."

On the other hand, Beaver teaches the abovementioned limitation (column 2, lines 60-64) as in systems providing revocable anonymity, anonymity is in place unless a specified event (e.g., court order) demands it be revoked and the identity of the offender revealed.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Beaver into the system of Teper, Camnisch, and Sako to prevent undesirable situations in which troublemakers can act without fear of detection.

11. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. (US 2002/0085713 A1).

With respect to claim 15, Feig teaches the limitations of "a first stage in which the client (C) calculates data formed of a series of tokens of which one enables a session to be opened and the others enable that session to be maintained", "a second stage in which the client (C) makes a strong undertaking to the server as to the series of tokens", and "a third stage of maintaining the session with the aid of the series of tokens." (page 1, paragraph 0005) as sending server

partitions the media file into a plurality of sequential data blocks. Thereafter, the server generates a plurality of cryptographic token keys, each token key corresponding to one of the plurality of sequential data blocks. Then the server encrypts each respective one of the plurality of sequential data blocks using a corresponding token key, thereby producing a plurality of the encrypted sequential data blocks. Then the server transfers the encrypted sequential data blocks to the client receiver. At the same time, the server transfers the plurality of token keys to the client receiver for immediate or later use.

It would have been obvious to one of the ordinary skill in the art at the time of the invention that the method described above can be applied to transferring data from any one machine to any other machine, therefore it can be used to transfer data from client to server.

12. Claim16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. (US 2002/0085713 A1) in view of Aiello et al. (US 6,397,329 B1).

It is noted that Feig does not explicitly teach the limitation of "the token generation step uses two cryptographic primitives, namely a hashing function and a random number"

On the other hand, Aiello teaches the abovementioned limitation (column 4, lines 51-52) as for a certificate that is valid for D days (or other time period), the random number is hashed D times.

In addition, examiner takes and Official Notice that the process of generating digital tokens and signatures through the use of one-way hash function applied to the random number is known in the art. Therefore, it would have been obvious to one of the ordinary skill in the art to incorporate teachings of Aiello into the system of Feig to generate the digital certificates.

13. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. (US 2002/0085713 A1) in view of Sako (US 2001/0011351 A1).

It is noted that Feig does not explicitly teach the limitation of "it uses a group signature by associating a plurality of identifiers and respective private keys with a single group public key."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0015) as the verification subsystem confirms that the data submitted has a signature verifiable by a group public key affixed and when the confirmation is obtained, this can be regarded as the data sent by a participant subsystem belonging to an eligible group.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Feig because use of the group signature makes it impossible to identify the particular participant in the group, which makes it possible to maintain anonymity.

With respect to claim 18, it is noted that Feig does not explicitly teach the limitation of "using a blind signature."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0005) as a participant subsystem authorized to vote proves before a manager subsystem that the presenter is authorized to vote and then has the manager subsystem sign the voting contents by section of blind signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Feig because since blind signature is used, even the manager subsystem cannot know to which participant subsystem the voting statement with the signature has been issued, which makes it possible to maintain anonymity.

14. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. (US 2002/0085713 A1) in view of Beaver et al. (US 7,234,059 B1).

With respect to claim 19, it is noted that Feig does not explicitly teach the limitation of "the powers to revoke anonymity are divided between two or more authorities"

On the other hand, Beaver teaches the abovementioned limitation (column 2, lines 60-64) as in systems providing revocable anonymity, anonymity is in place unless a specified event (e.g., court order) demands it be revoked and the identity of the offender revealed.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Beaver into the system of Feig to prevent undesirable situations in which troublemakers can act without fear of detection.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. Newcombe (US 2003/0172269 A1).

b. Williams (US 2003/0005118 A1).

c. Gudbjartsson et al. (US 2001/0027519 A1).

d. Harif (US 2002/0087473 A1).

e. Sprague (US 2003/0014631 A1).

f. Kou (US 6,363,365 B1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 8:30 - 18:00, Fri 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/ 9/10/2008
Examiner, Art Unit 2131

/Syed Zia/
Primary Examiner, Art Unit 2131